EXHIBIT B

NON-STATUTORY OBVIOUSNESS –TYPE DOUBLE PATENTING

PATENT L.R. 3-3(B)

U.S. Patent No. 6,654,884 to Jaffe et al.

'661 Patent, Claim 6	**U.S. Patent No. 6,654,884 to Jaffe et al.**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising An input interface is inherent in devices performing cryptographic operations.
(b) a source of unpredictable information;	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising
(c) a processor:	Claim 1 – (a) a processing circuit
(i) connected to said input interface for receiving and cryptographically processing said quantity,	Claim 1 – (a)(i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.

additional electricity in said microchip during said processing; and	
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	An output interface is inherent in devices performing cryptographic operations.

'661 Patent, Claim 11	**U.S. Patent No. 6,654,884 to Jaffe et al.**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum An input interface is inherent to devices performing cryptographic operations.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum

(d) a noise production system for introducing noise into said measurement of said power consumption.	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.

'661 Patent, Claim 12	**U.S. Patent No. 6,654,884 to Jaffe et al.**
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(b) a noise processing module for improving the random characteristic of said initial noise; and	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.

'661 Patent, Claim 23	**U.S. Patent No. 6,654,884 to Jaffe et al.**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising

(b) generating unpredictable information;	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between:	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum
(c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and	Claim 1 – (b) balancing circuitry, configured (i) to operate concurrently with said processing circuit, and (ii) such that power consumption of said balancing circuitry varies depending on said input datum in a direction complementary to said variation in said power consumption of said processing circuit Claim 2 – The device of claim 1 where said balancing circuitry includes a plurality of logic subunits configured to have an input-dependent power consumption that is complementary to power consumption of said subunits in said processing circuit. Claim 3 – The device of claim 2 configured so that results of said balancing circuitry are discarded and do not affect a result of said cryptographic operation.
(d) outputting said cryptographically processed quantity to a recipient thereof.	Outputting a value is inherent to devices performing cryptographic operations.

'661 Patent, Claim 25	U.S. Patent No. 6,654,884 to Jaffe et al.
The method of claim 23 where said selecting is performed in hardware on an integrated circuit including a microprocessor.	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum Claim 1 – (b) balancing circuitry, configured (i) to operate concurrently with said processing circuit, and (ii) such that power consumption of said balancing circuitry varies depending on said input datum in a direction complementary to said variation in said power consumption of said processing circuit Claim 2 – The device of claim 1 where said balancing circuitry includes a plurality of logic subunits configured to have an input-dependent power consumption that is complementary to power consumption of said subunits in said processing circuit.

'661 Patent, Claim 29	U.S. Patent No. 6,654,884 to Jaffe et al.
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	Claim 1 - A cryptographic processing device for securely performing a cryptographic processing operation on an input datum in a manner resistant to discovery of a secret by external monitoring of consumed power, comprising
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies depending on said input datum
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a	Claim 1 – (a) a processing circuit (i) including a plurality of logic subunits configured to compute at least a portion of a cryptographic operation (ii) where power consumption of said circuit varies

portion of a message;	depending on said input datum
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(d) outputting said cryptographically processed quantity to a recipient thereof.	Outputting a value is inherent performing cryptographic operations.

'661 Patent, Claim 30	**U.S. Patent No. 6,654,884 to Jaffe et al.**
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(b) improving the random characteristic of said initial noise; and	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.
(c) varying said power consumption based on said improved initial noise.	Claim 1 – (c) an unpredictable noise source configured to mask information leaked in power consumption of said device by causing variations in said power consumption uncorrelated to operation of said processing circuit.

U.S. Patent No. 6,381,699 to Kocher et al.

'661 Patent, Claim 6	**U.S. Patent No. 6,381,699 to Kocher et al.**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery	Claim 1 – A cryptographic token configured to perform cryptographic operations using a secret key in a secure manner, comprising: Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination

of a secret by external monitoring, comprising:	of said secret key infeasible from external measurements of said power consumption characteristic Claim 2 – The cryptographic token of claim 1, in the form of a secure microprocessor.
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	An input interface is inherent to a secure microprocessor device for performing cryptographic operations.
(b) a source of unpredictable information;	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(c) a processor:	Claim 1 – (c) a processor:
(i) connected to said input interface for receiving and cryptographically processing said quantity,	An input interface connected to the processor is inherent to a secure microprocessor device performing cryptographic operations.
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	Claim 1 – (a) an interface configured to receive power from a source external to said token Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	An output interface is inherent to a secure microprocessor device performing cryptographic operations.

'661 Patent, Claim 11	U.S. Patent No. 6,381,699 to Kocher et al.
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	Claim 1 – A cryptographic token configured to perform cryptographic operations using a secret key in a secure manner, comprising: Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	An input interface is inherent to a device performing cryptographic operations.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	Claim 1 – (a) an interface configured to receive power from a source external to said token Claim 1 – (d) said token having a power consumption characteristic: (i) that is externally measurable; and (ii) that varies over time in a manner measurably correlated with said cryptographic operations
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	Claim 1 – (c) a processor: Claim 1 – (c)(ii) configured to perform said processing using said secret key from said memory An input interface is inherent to a device performing cryptographic operations.
(d) a noise production system for introducing noise into said measurement of said power consumption.	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.

'661 Patent, Claim 12	U.S. Patent No. 6,381,699 to Kocher et al.
The device of claim 11 wherein said noise production system comprises: (a) a source	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of

of randomness for generating initial noise having a random characteristic;	said power consumption characteristic.
(b) a noise processing module for improving the random characteristic of said initial noise; and	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.

'661 Patent, Claim 22	**U.S. Patent No. 6,381,699 to Kocher et al.**
A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	Claim 3 – The cryptographic token of claim 1, in the form of a smart card.

'661 Patent, Claim 23	**U.S. Patent No. 6,381,699 to Kocher et al.**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	Claim 1 – A cryptographic token configured to perform cryptographic operations using a secret key in a secure manner, comprising: Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	An input/output interface is inherent to devices performing cryptographic operations.
(b) generating unpredictable information;	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said

	power consumption characteristic.
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between:	Claim 1 – (c)(ii) configured to perform said processing using said secret key from said memory Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and	Claim 1 – (c)(ii) configured to perform said processing using said secret key from said memory Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and	Claim 1 – (c)(ii) configured to perform said processing using said secret key from said memory Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(d) outputting said cryptographically processed quantity to a recipient thereof.	An input/output interface is inherent to devices performing cryptographic operations.

'661 Patent, Claim 25	**U.S. Patent No. 6,381,699 to Kocher et al.**
The method of claim 23 where said selecting is performed in hardware on an integrated circuit including a microprocessor.	Claim 2 – The cryptographic token of claim 1, in the form of a secure microprocessor.

'661 Patent, Claim 29	U.S. Patent No. 6,381,699 to Kocher et al.
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	Claim 1 – A cryptographic token configured to perform cryptographic operations using a secret key in a secure manner, comprising: Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	Claim 1 – (a) an interface configured to receive power from a source external to said token Claim 1 – (d) said token having a power consumption characteristic: (i) that is externally measurable; and (ii) that varies over time in a manner measurably correlated with said cryptographic operations
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	Inherent for a cryptographic operation to receive a message to be processed.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	Claim 1 – (c) a processor: Claim 1 – (a) an interface configured to receive power from a source external to said token Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(d) outputting said cryptographically processed quantity to a recipient thereof.	Inherent for cryptographic operation to output a processed quantity.

'661 Patent, Claim 30	U.S. Patent No. 6,381,699 to Kocher et al.
The method of claim 29	Claim 1 – (e) a source of unpredictable information configured

wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(b) improving the random characteristic of said initial noise; and	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.
(c) varying said power consumption based on said improved initial noise.	Claim 1 – (e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key infeasible from external measurements of said power consumption characteristic.